System Safety and Reliability Modeling for the Next Generation of Air Transportation

Vitali Volovoi
School of Aerospace Engineering Georgia Tech
E-mail vitali@gatech.edu

NASA Statistical Engineering Symposium

Williamsburg, Virginia

May 5 2011

Risks and hazards of the second order

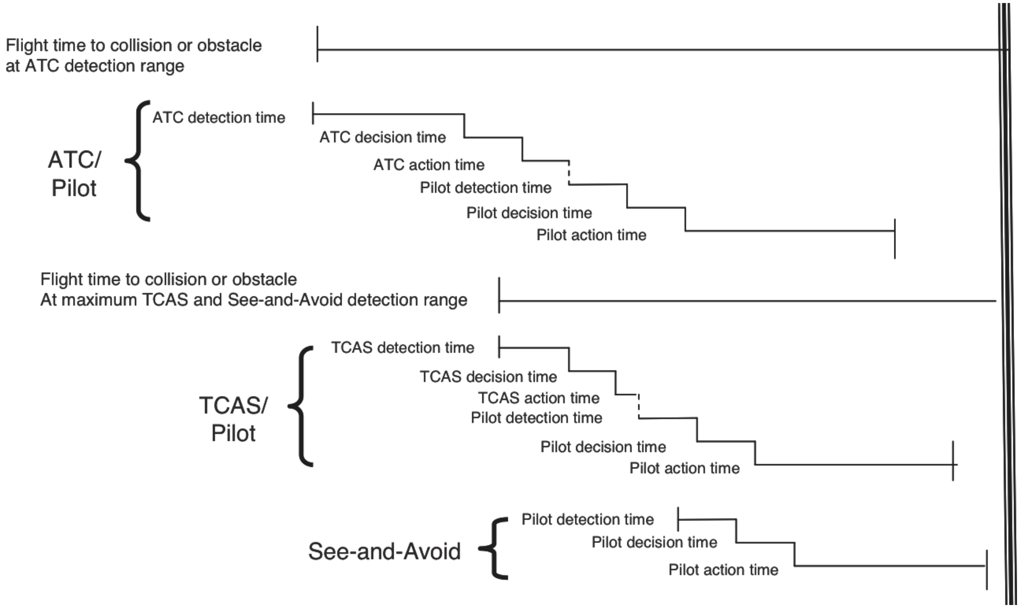
- **Two extremes – the same conclusion:**
  - Existing tools are sufficient and do just fine in modeling safety, so no further research is needed
  - Problems are so complex that there is no point of dealing with them now (we cross the bridge when we come to it)
- **Extensive specific domain knowledge is required as the underlying processes are unique and involved**
- **There is a lack of cohesion in engineering and scientific community making it difficult to ensure that safety issues are adequately addressed**
- **This undercuts the trust from the decision makers (negative feedback loop):**
  - The decision makers do not invest in system safety problems
  - So the community further dissolves

Background

- **Existing approaches to assessing system-level safety:**
  - At the vehicle level: fault-trees and reliability block diagrams FAA certification following ARP4761
  - At the ATC level: combination of fault-trees and event-trees. Similar to Probabilistic Risk Assessment (PRA) used in Nuclear and NASA Space program
- **Both of those existing approaches decouple temporal (event trees or their equivalent) from logical complexity (fault trees or their equivalent)**
- **ATC operations exhibit highly coupled behavior between the temporal and logical domain, and this coupled behavior must be modeled at the bottom level using physics-based simulation**
- **There are two issues with modeling coupled failure behavior at the bottom level:**
  - Breadth vs. depth trade-off in complexity – those simulations are really good depth-wise, not so good from the breadth viewpoint
  - Focus is on the simulation of the operation, rather than on paths and logic of failure propagation

Coupling of timing and logic complexity

- **Timing is important! Static tools (fault trees) cannot capture the timing effects**
- **Simulation with 4-D trajectories is possible, but not practical as the control logic gets more and more complicated (the breadth issue)**

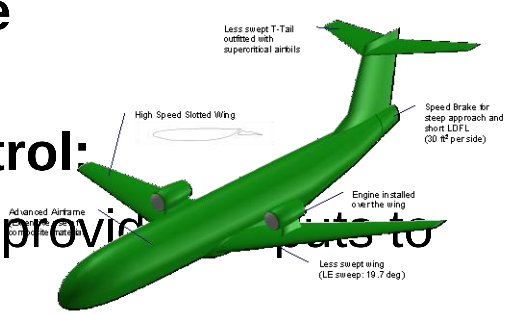


Redundancy of space conflict resolution in current NAS (R. Hemm and A. Busick, ATIO 2009)

- **Stochastic Petri Nets (SPNs) are suggested as an intermediate layer of analysis. Nested analysis is modular (unlike integrated application of SPN to safety of spacing separation– H. Blom et al, ATIO 2007)**
- **Succinct representation: compact discrete state-space and continuous time (more complex is not always better)**

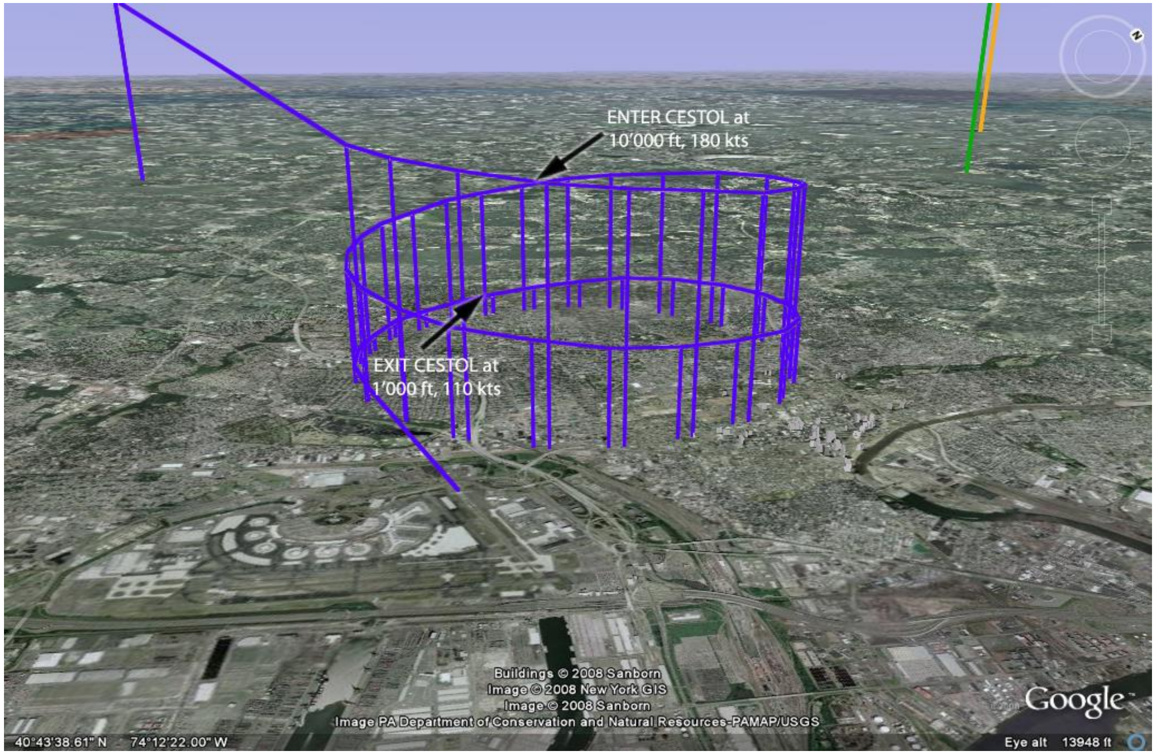
Credible Hazard Scenario for CESTOL

- **Cruise efficient short takeoff and landing CESTOL**
- **Spiral/Helix approach**
- **Impact of wind (steady-state and gust) on the trajectory in the regime of manual control**
- **Potential triggers of reverting to manual control:**
  - Generator/electrical failure of the equipment provid[illegible]puts to FMS
  - Loss of navigational inputs to FMS or degraded state of FMS itself
- **Motivation (potentially exacerbating factors)**
  - Changing heading (changing relative influence of the wind)
  - CESTOL low wing loading – more susceptible to wind disturbances


Less swept T-Tail outfitted with supercritical airfoils
High Speed Slotted Wing
Speed Brake for steep approach and short LDFL (30 ft² per side)
Engine installed over the wing
Advanced Airframe (Extensive use of composite material)
Less swept wing (LE sweep: 19.7 deg)

Spiral/Helix

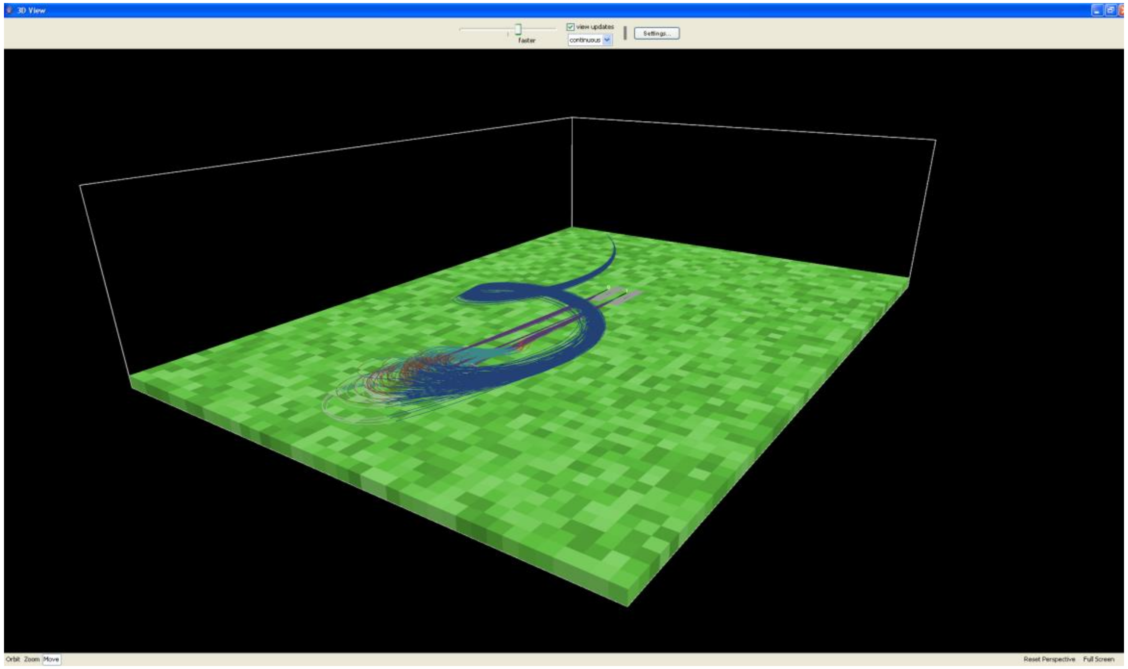
- Spiral descent originally used as noise abatement
- Moved off-airport to allow for stabilization maneuver
- Bank angles was allowed to vary and instead the radius is kept constant (helix)



Descent Helix for CESTOL (Image of Air Transportation Lab at Georgia Tech)

Agent-Based Simulation of using NetLogo

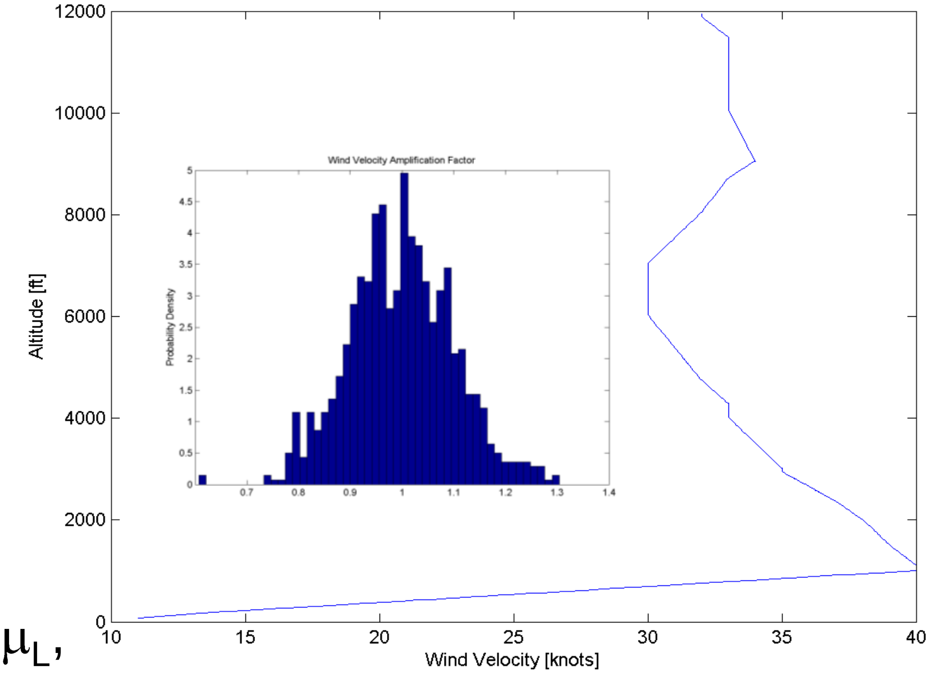
- NetLogo has been developed at Northwestern University, has good interface with other pre- and post-processing software (Matlab, Mathematica)
- Main Parameters: geometry, wind, pilot response delay



NetLogo model 500 random trajectories

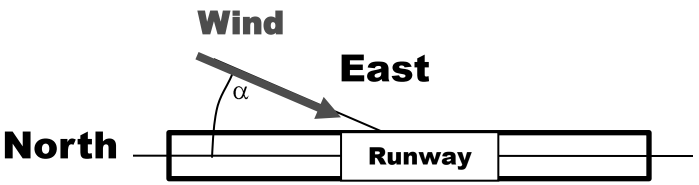
Simulation assumptions

- **Uncertainty Sources:**
  - Pilot’s response delay
  - Forecast error (wind direction and intensity)
- **Assumptions:**
  - Rescaling & rotation of nominal wind according to Gaussian distribution ~*N*(μ, σ)
  - Lognormal pilot’s response ~ *L*(μ_L, σ_L) (not to exceed 20 sec)
- **Probability of minimum distance violation**



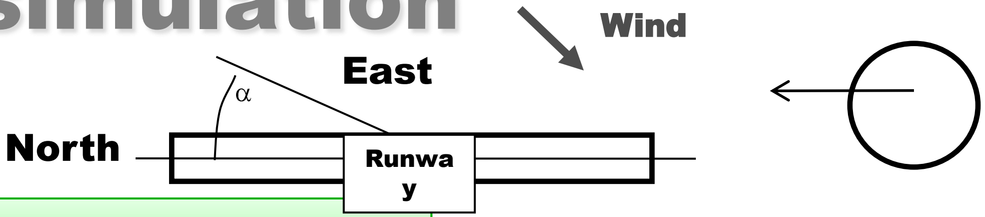
Focus of the model

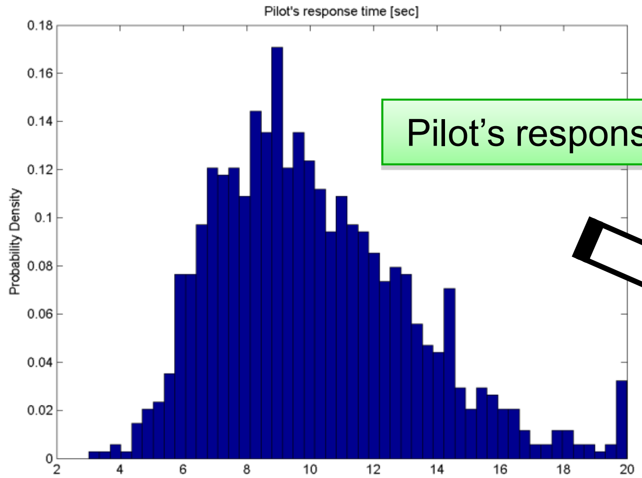
$$P_{violation} = P_{failure\_fms} \times P_{helix\_drift} \times P_{other\_aicraft}$$



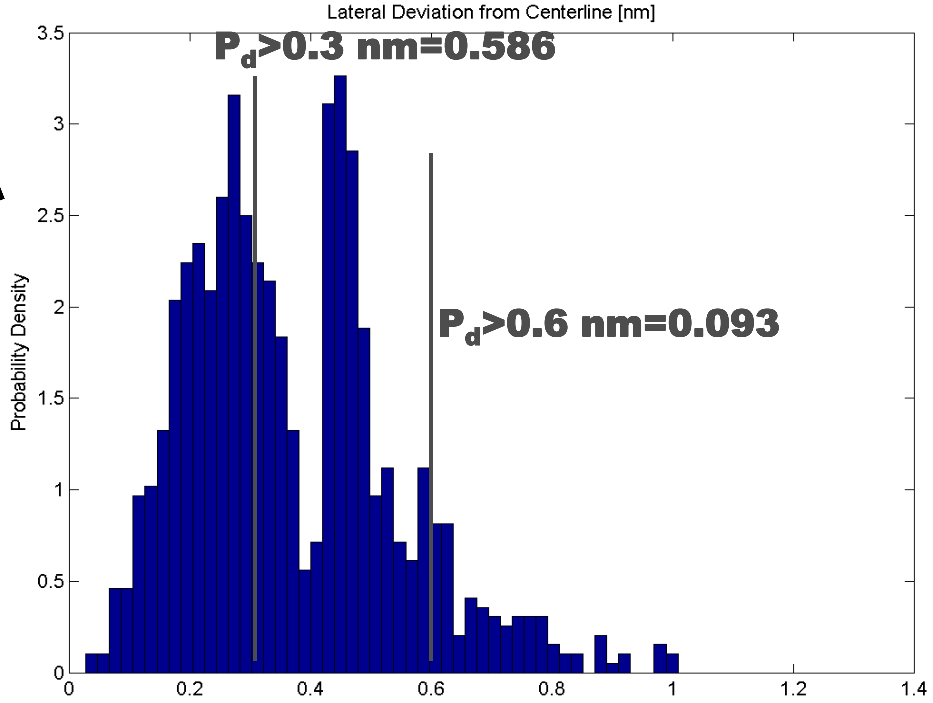
In general, things are a bit more complicated (timing is important)

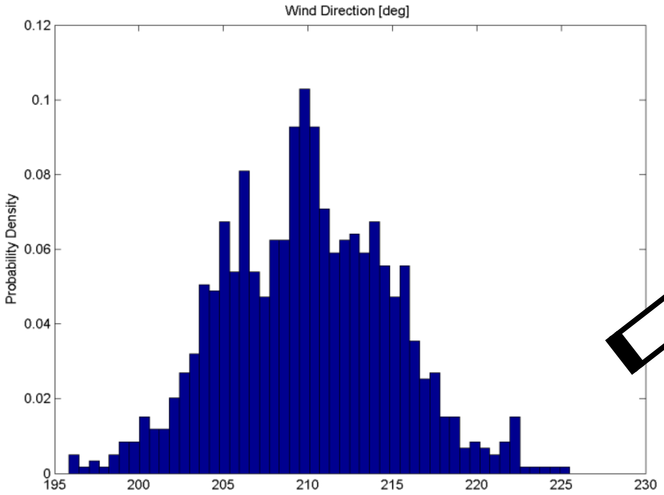
Results from agent-based simulation





Pilot’s response time ~ L(μ_L=10 sec, σ_L=10 sec)



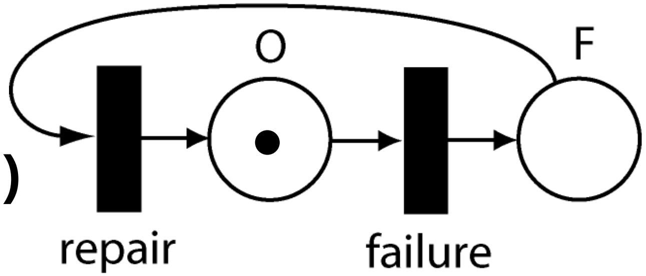


Wind intensity’s amplification factor ~ N(μ=1, σ = 0.1)
Error in wind direction ~ N(μ=0°, σ= 5°)

Georgia Institute of Technology

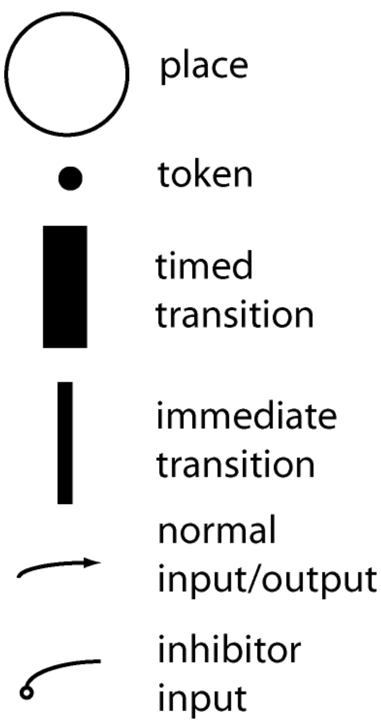
Introducing Stochastic Petri Nets

- Tokens represent relevant entities of a modeled system
- Places represent possible states of those entities
- Tokens occupy places, thus realizing particular states of the corresponding entities
- The combination of all tokens' locations (so-called marking) uniquely characterizes the modeled system
- Tokens move between places, simulating changes in the system state
- Transitions describe the rules for token movements: tokens are "fired" from one place to another via transitions
- Transitions fire only when they are enabled (i.e., if certain conditions are satisfied)
- Transitions are enabled based on where other tokens are thus capturing interdependence among components states (inhibitors are used)
- An enabled transition fires after a specified delay (the transition's attribute)



A repairable unit

Notations:



SPN@:
Implementation of SPN with aging tokens

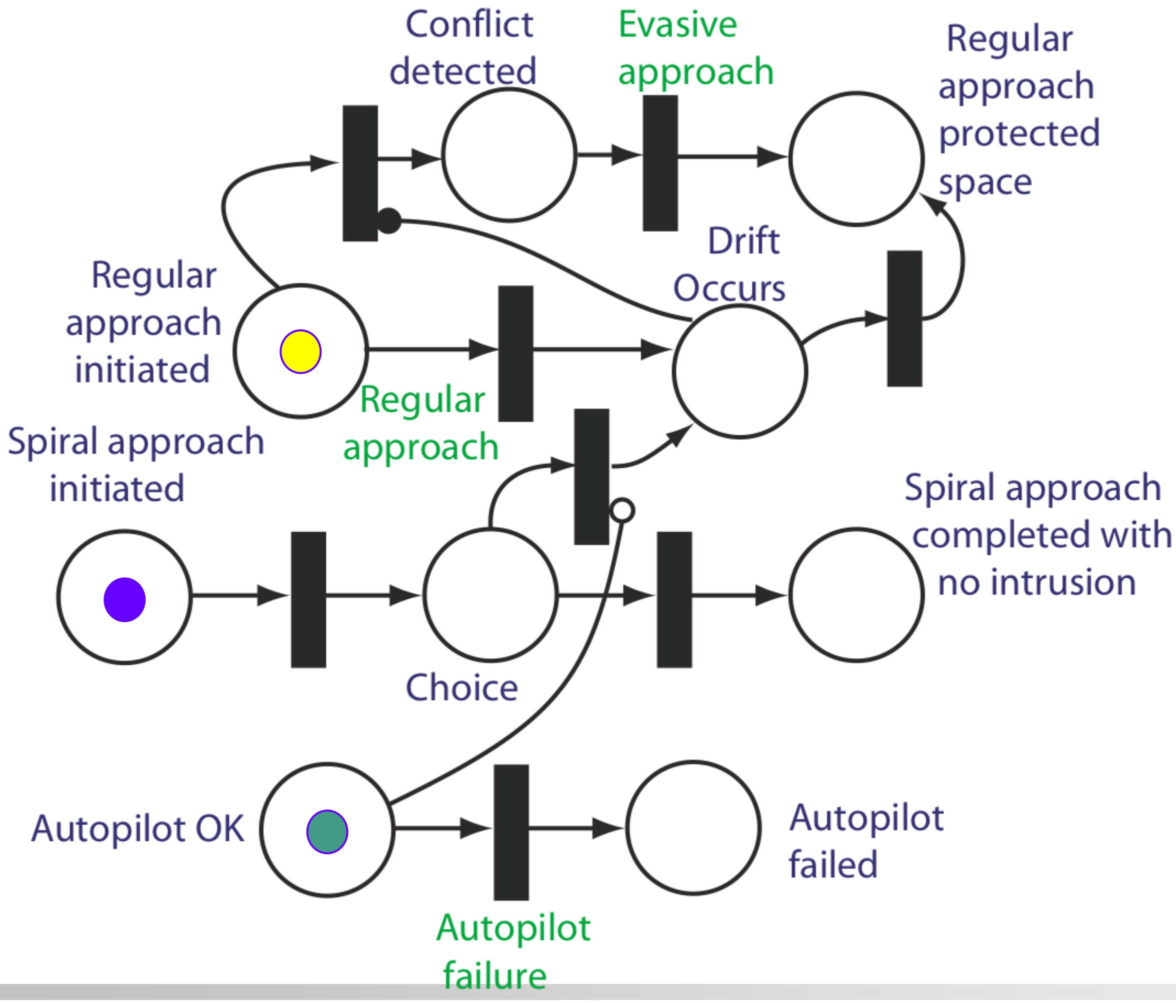
Version 0.38 (Feb 1, 2010)

For more information
please contact
Dr. Vitali Volovoi
vitali.volovoi@ae.gatech.edu
tel. (404) 894-9811

SPN @

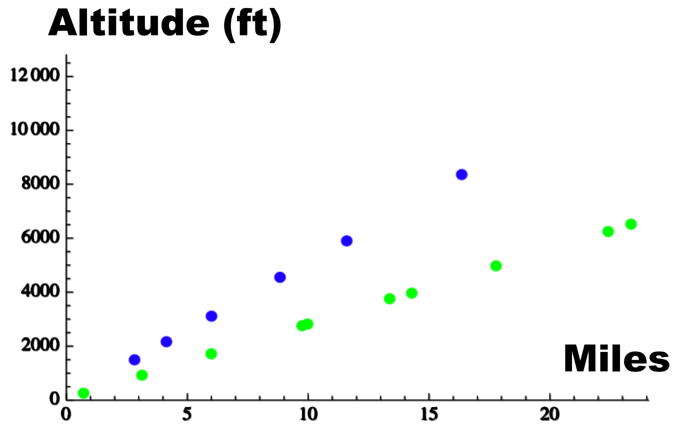
This product is licensed for educational
and evaluational purposes only

Modeling of separation violation at a higher level of abstraction using SPN


Conflict detected
Evasive approach
Regular approach protected space
Drift Occurs
Regular approach initiated
Regular approach
Spiral approach initiated
Spiral approach completed with no intrusion
Choice
Autopilot OK
Autopilot failed
Autopilot failure

A Hazard Scenario from VLJ

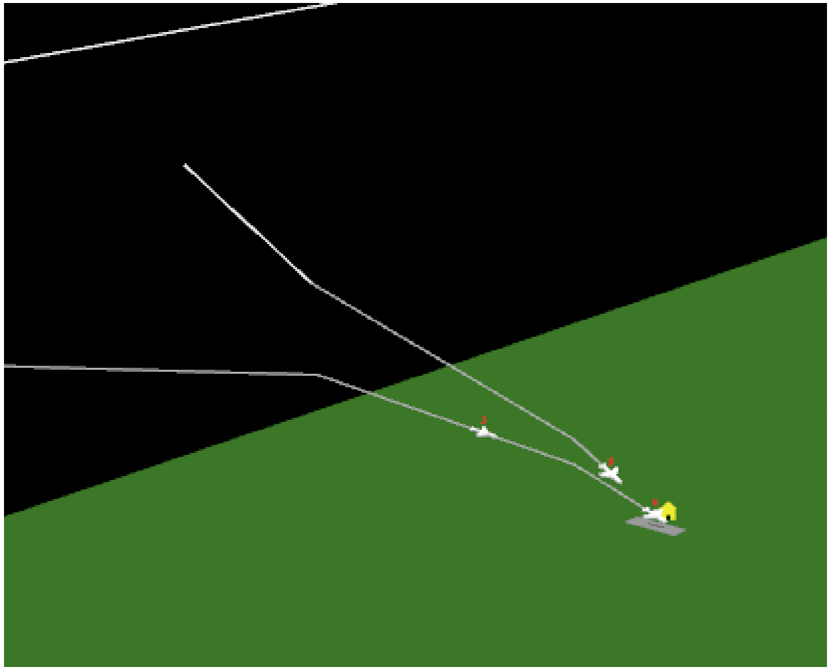
- Very Light Jet on a straight steep (5.5 degree) approach mixed with two regular aircraft loses capability to evaluate the altitude (e.g., Pitot tube obstruction resulting in corruption of air data) and starts to descent faster than intended thus potentially leading to vertical space violation with the leading aircraft



- ATC notices the impending loss of separation and orders leveling off
- If VLJ is not responding after a certain amount of time the leading aircraft is ordered to speed up the descent
- Single pilot vs. two pilots (remote co-pilot)
- Motivation – importance of accommodating mixed approach with various descent speed by means of vertical separation
- Motivation – importance of investigating the viability of a back-up pilot on the ground

Challenges of modeling VLJ

- Standard load-sharing by pilots (where in the case of emergency one pilot flies and the other trouble-shoots the problem and communicates with ATC) is not applicable when one of the pilots is on the ground
- As a result, the co-pilot on the ground is assumed to have the same capabilities as the VLJ pilot



Snap Shot of NetLogo model of VLJ

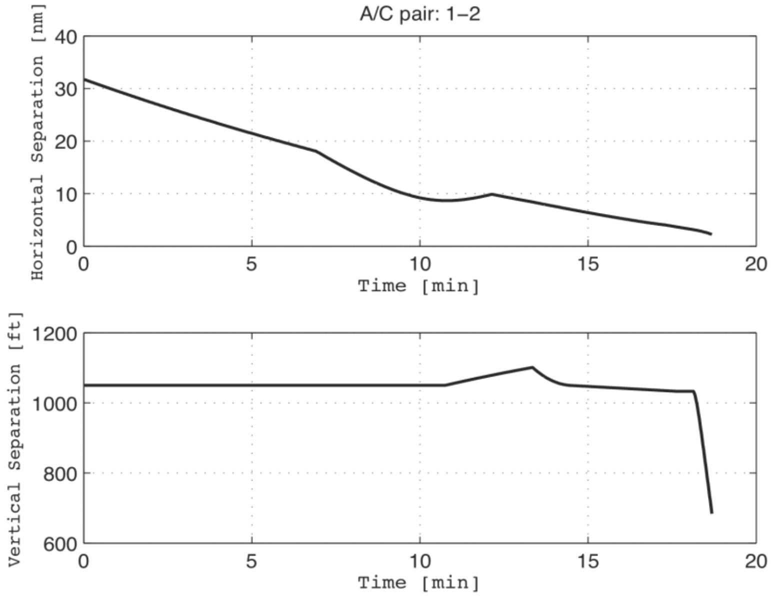
- We assume that pilots share the load, thus conducting tasks faster (up to twice as fast). When ATC sends the command, the current task is completed, and then ATC command is executed

Pilot Tasks breakdown and their duration

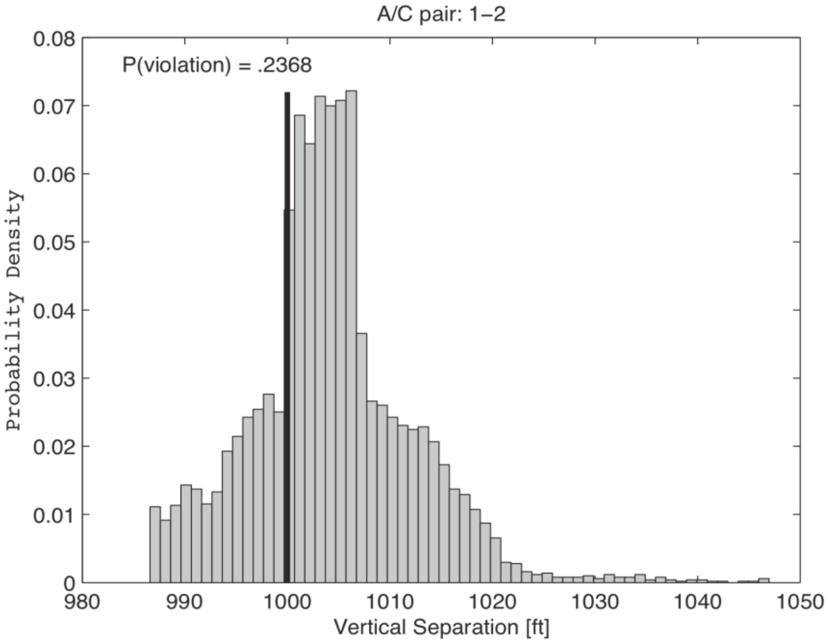
Phase of flight	Task	Average time to accomplish (mins)	STD
Prior to Top of Descent	Check Weather	2.5	0.65
	Check fuel state	0.5	0.158
	Check altimeter setting	0.5	0.149
	Check FMS programming	1	0.3
	Select radio frequencies	0.5	0.176
	Review Approach Plate	1	0.25
	Receive Approach Clearance [ATC communication]	varies depending on clearance	
	Set DH or MDA into Radar Altimeter	0.25	0.017
	Select landing gear down	instantaneous	
Top of Descent	Monitor Descent Progress	throughout descent (every 1 min)	
	Instrument scan	throughout approach (every 10 secs)	
	Monitor aircraft systems	throughout flight (every 1 min)	
	Frequency Change	0.25	0.015
	Check RAIM [GPS satellite coverage]	0.25	0.027
	Check aircraft configuration	0.25	0.046
Final Approach Fix	Report FAF [contact ATC]	0.25	0.037
	Scan for runway environment	intermittent from FAF to landing	
	Verify landing clearance [contact ATC]	0.1	0.056
	Wind check [contact ATC]	0.25	0.025
DH/MDA	Verify runway environment IAW (FAR 91.175)	until touchdown	
If runway environment is not insight			
Missed Approach	Execute missed approach instructions	depends on instructions	
	select TO/GA	instantaneous	
	Clean-up aircraft (manually)	2	0.8
	Report missed approach [contact ATC]	0.1	0.015

Sample results for VLJ

- Pair-wise separation is studied when the faults are inserted at different altitudes (1000 cases of Monte Carlo agent based simulation)

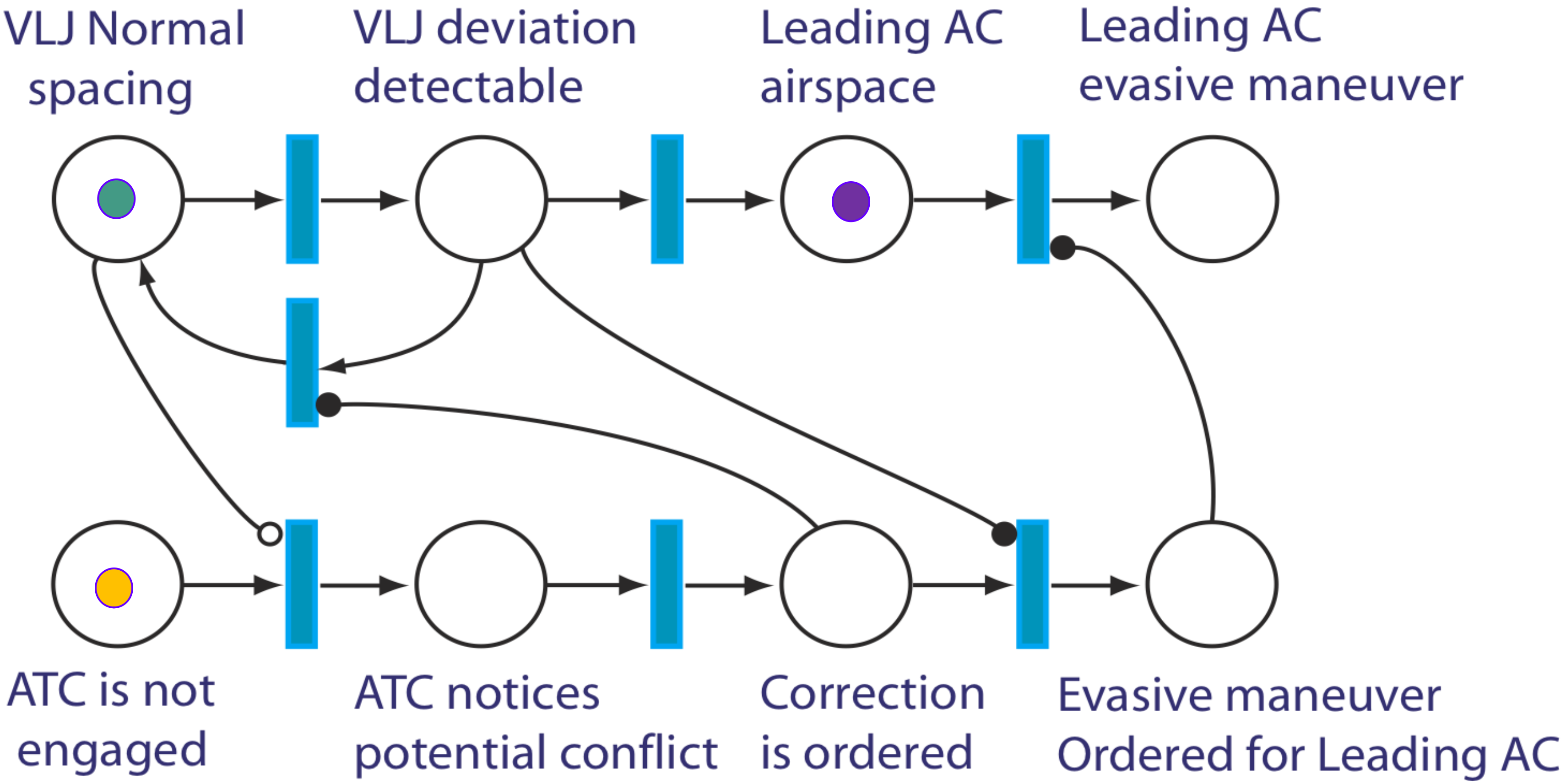


Tracking pair-wise horizontal and vertical separation

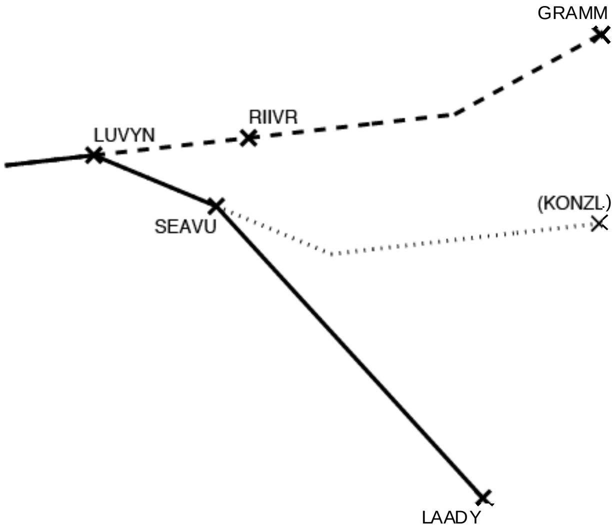


Probability of the loss of vertical separation
1-2 aircraft, loss of VNAV at 5000ft

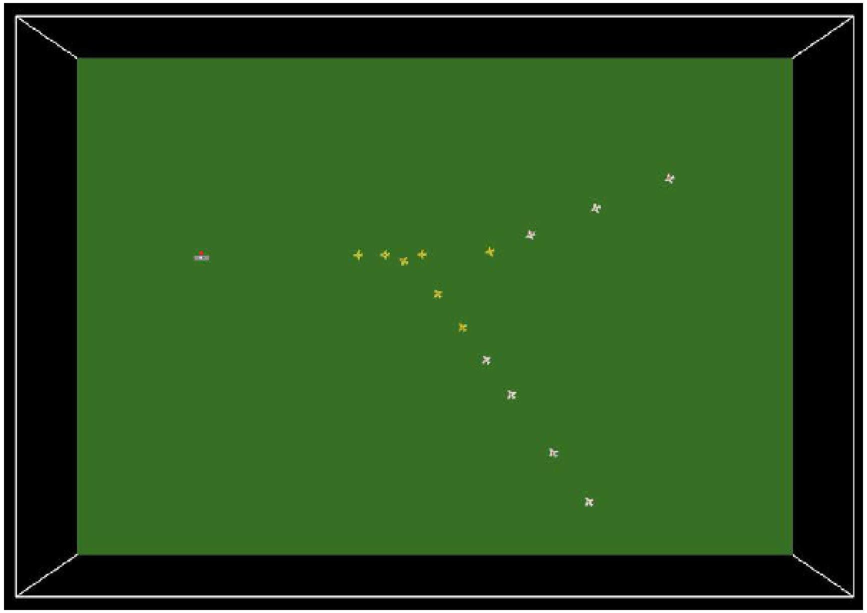
SPN: VLJ Hazard Scenario



Merging aircraft with optimized descent profile in LAX



Schematics of merging routes

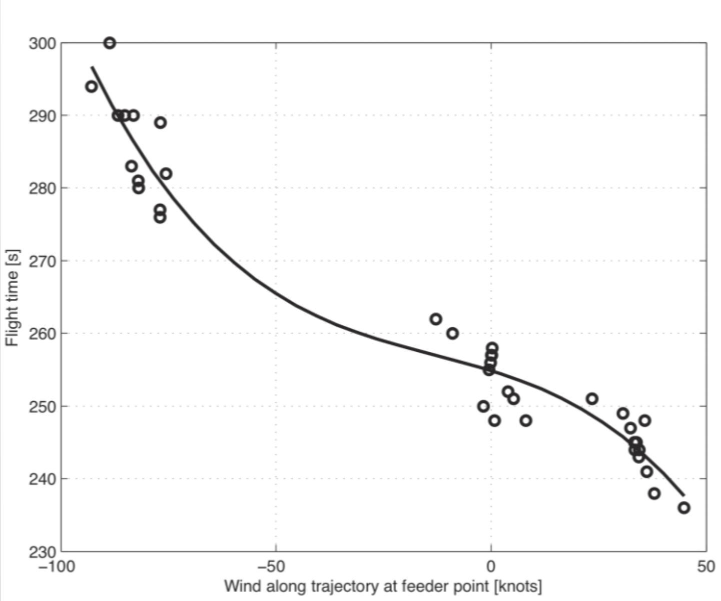


Agent-based simulation (Netlogo snapshot)

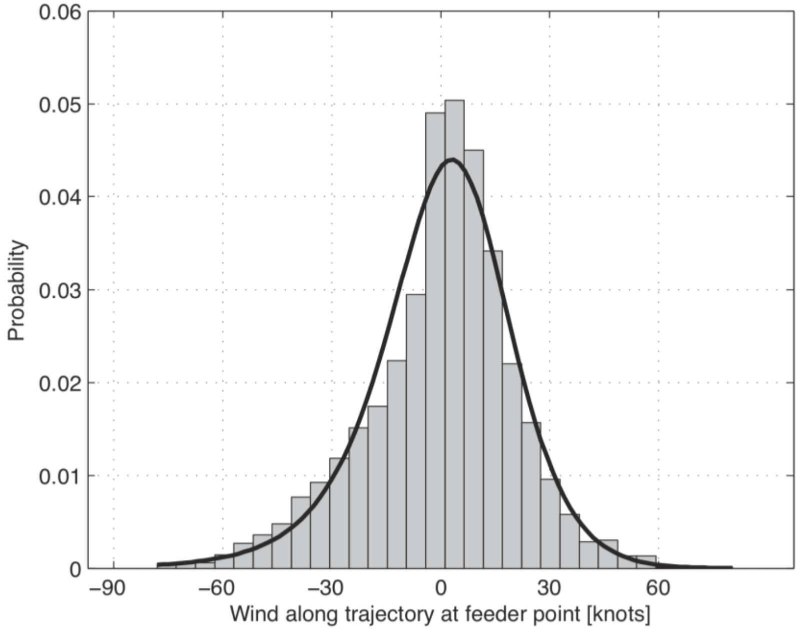
Only a portion of operational procedures in modeled in this example (no vectoring, acceleration or, coordinated conflict is modeled), only two air traffic fluxes are considered

Merging aircraft with optimized descent profile

Optimized descent profile (also referred to as continuous descent) is implemented in LAX – has fuel efficiency and noise benefits but introduces uncertainty in traveling time due to wind

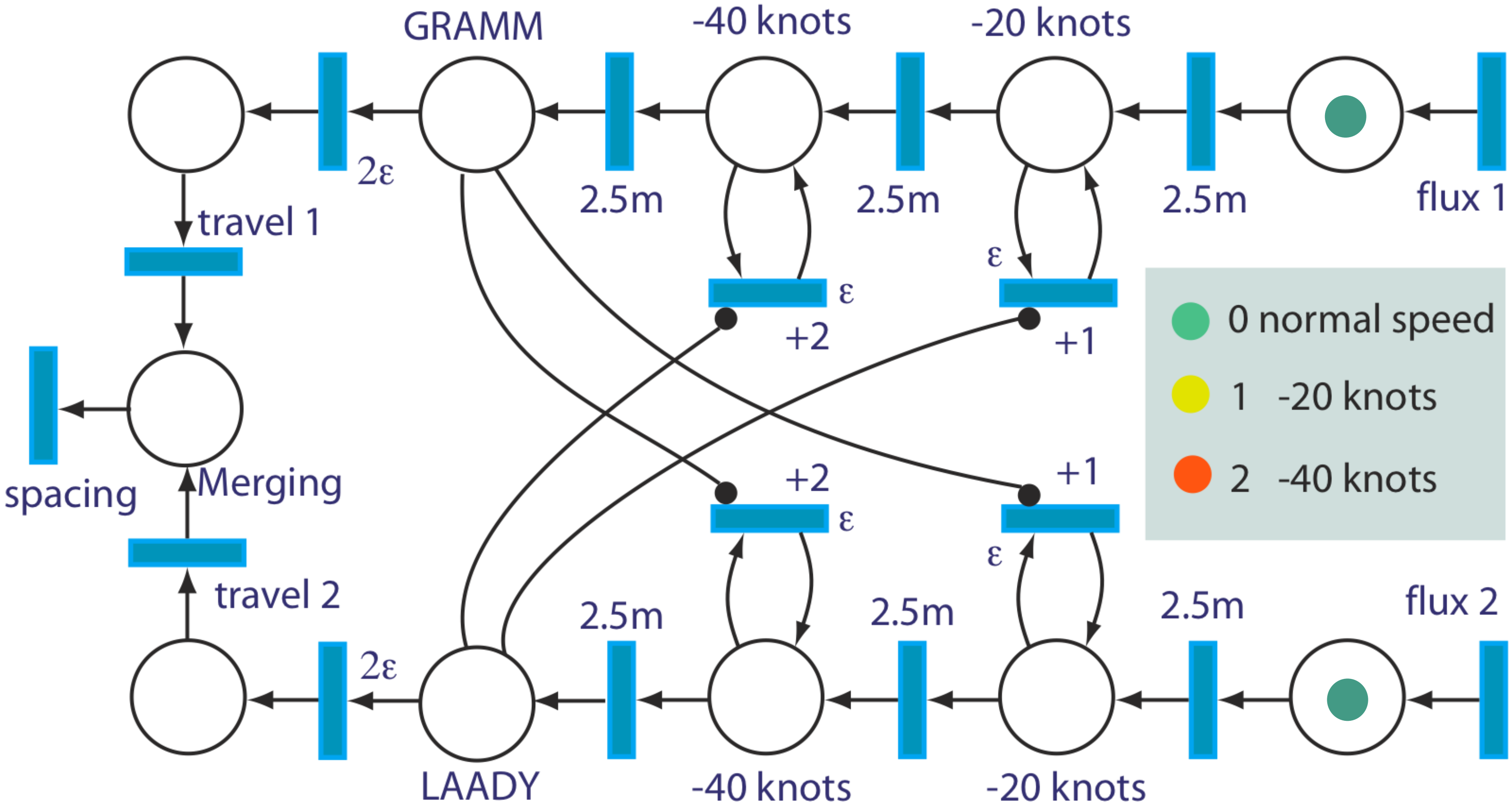


Flight time to merging point as a function of the wind – not that is non-linear!



Wind distribution (as observed)

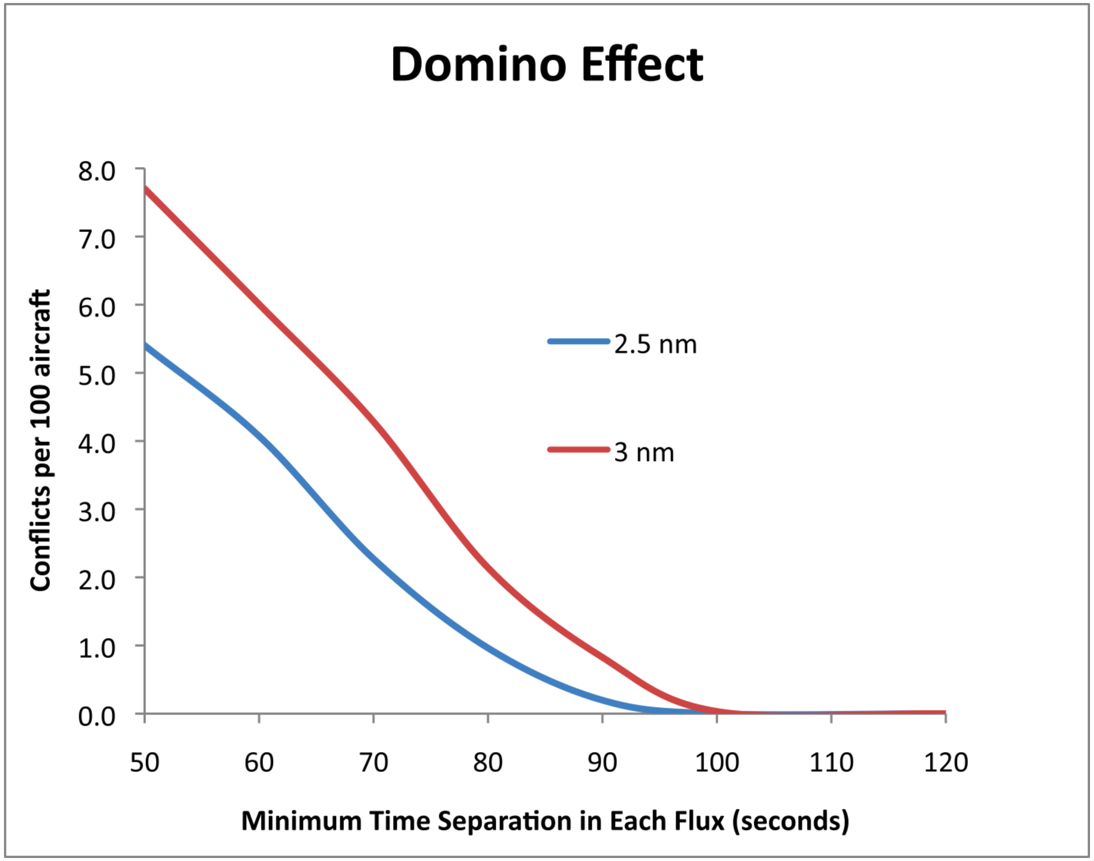
Merging aircraft OPD in LAX – SPN model



● 0 normal speed
● 1 -20 knots
● 2 -40 knots

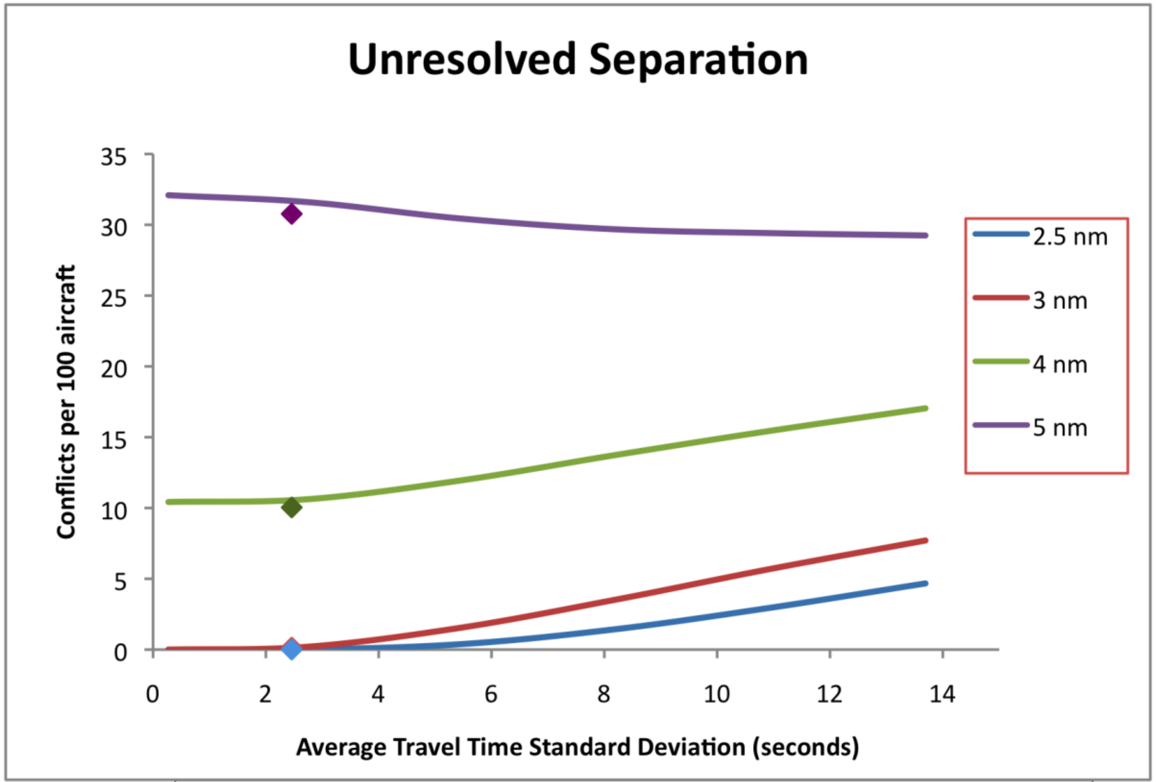
Tokens represent aircraft that change colors in accordance with the ordered maneuvers. Statistics are collected about the conflicts at the merging point (when two tokens are together)

Sample of results from SPN – efficiency of the maneuvers (unresolved conflict frequency)



Frequency of spacing violations as a function of a minimum separation within each flux (no wind is considered)

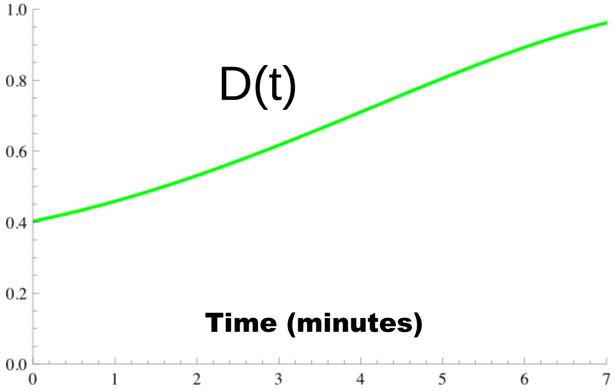
Sample of results from SPN – efficiency of the maneuvers (unresolved conflict frequency)



Sensitivity of the maneuver efficiency as a function of the travelling time uncertainty (diamonds represent the results of global agent-based simulation for modeled wind)

Safety Analysis of the Advanced Airspace Concept: State space representation

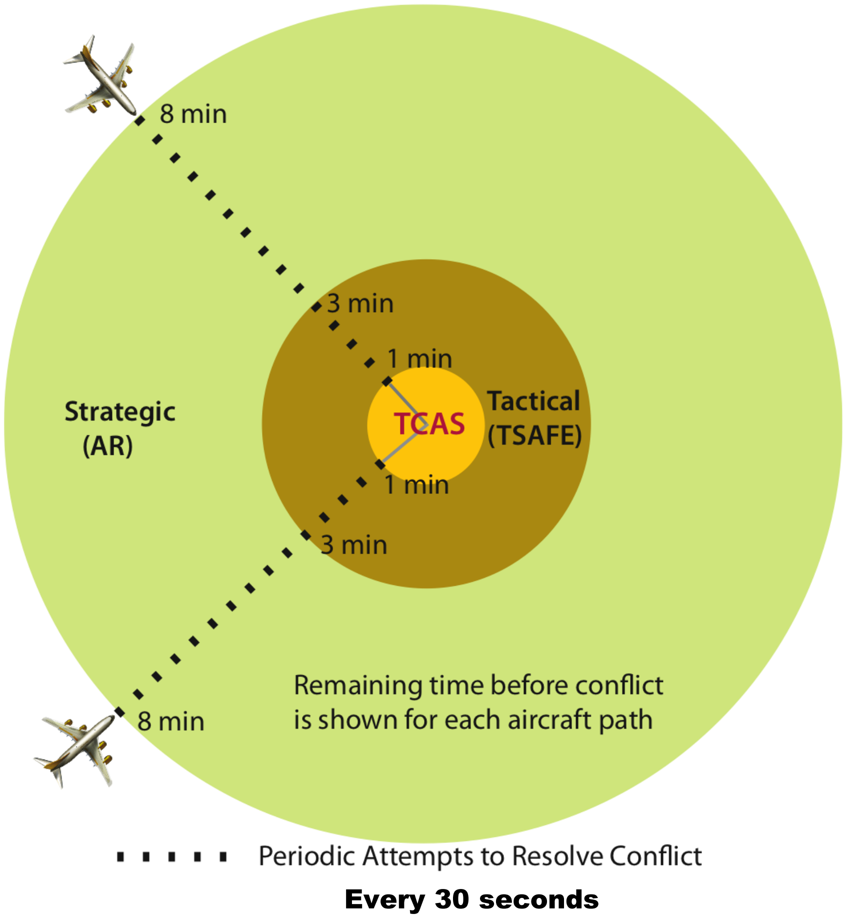
Probability of Conflict Detection



Three layers of automation:

1. Autoresolver (AR) – from 8-20 to 3 min before the conflict
2. Tactical Separation-Assured Flight Environment (TSAFE) 1-3 min before the conflict
3. TCAS – 1 min

+ visual avoidance

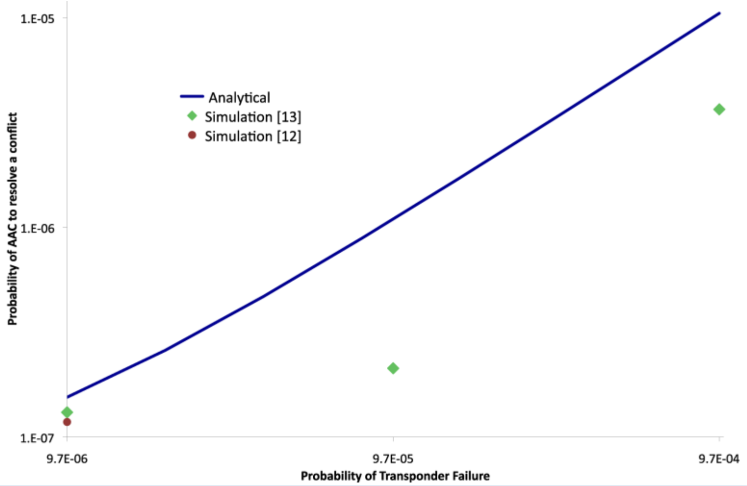


Remaining time before conflict is shown for each aircraft path

▪ ▪ ▪ ▪ ▪ Periodic Attempts to Resolve Conflict

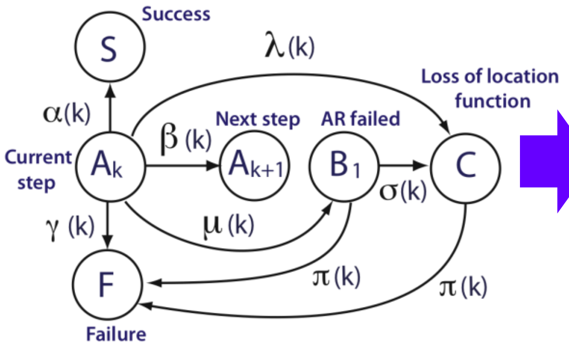
Every 30 seconds

Safety Analysis of the Advanced Airspace Concept: State space representation

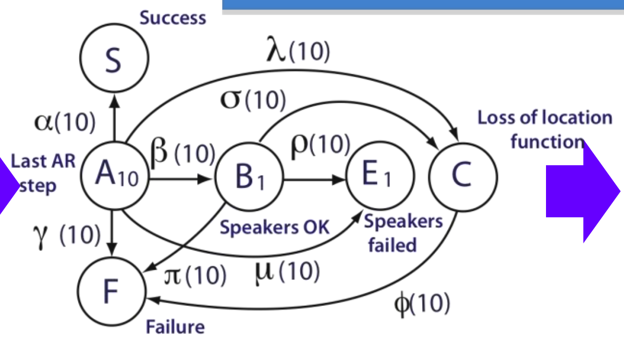


Probability of Sub-system failure is increasing with time, and different layers share common subsystems:
T – transponders (all three layers)
L – location function (AR and TSAFE)
K – speakers TSAFE and TCAS,
in addition subsystems specific to each layer also can fail (A, B, C for AR, TSAFE, and TCAS, respectively

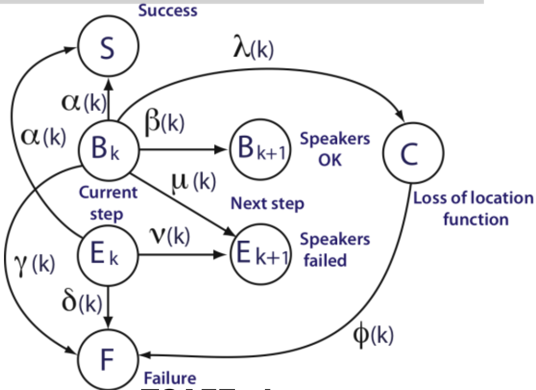
Analytical procedure is developed it Includes modeling of dependent subsystems (by semi-inverting Markov model for non-repairable portions of the system)



AR phase
(time steps 1-9)



AR to TSAFE transition
(time steps 10)



TSAFE phase
(time steps 11-15)

Conclusions

- **Complexities of modeling safety aspects of NextGen should not prevent us from trying our best, as neglecting those aspects will lead to dire consequences**
- **Agent-based simulation provide a useful environment to investigate combined effects of NextGen, procedures, and vehicle characteristics (analogous to physics-of-failure modeling in reliability), but they have their limitations**
- **While realistic logic branching can be modeled using agent-based simulation, a more compact modeling at a higher level of abstraction is beneficial at the very least**
- **Nested hierarchy of models is required for comprehensively assessment of the safety of new vehicle integration into NextGen**
  - Most detailed level: agent-based and simulations of perturbations of 4-D trajectory as well as detailed human-performance models (including Human-in-the-loop simulations of specific scenarios)
  - Intermediate level: Stochastic Petri Nets or analogous discrete-event simulation captures timing event, but provides discrete state-space representation. Markov chains if possible
  - Top level: Fault Tree and similar Boolean Algebra tools